

Tilburg University

## Zorgplichten van banken tegen DDoS-aanvallen

Tjong Tjin Tai, T.F.E.

*Published in:*  
Nederlands Juristenblad

*Publication date:*  
2013

*Document Version*  
Publisher's PDF, also known as Version of record

[Link to publication in Tilburg University Research Portal](#)

*Citation for published version (APA):*  
Tjong Tjin Tai, T. F. E. (2013). Zorgplichten van banken tegen DDoS-aanvallen. *Nederlands Juristenblad*, 88(32), 2196-2200.

### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

### Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# Zorgplichten van banken tegen DDoS-aanvallen

Eric Tjong Tjin Tai<sup>1</sup>

Als internetbankieren uitvalt wegens een DDoS-aanval is er wellicht wel een mogelijkheid om bij banken claims in te dienen voor schadevergoeding, maar de omvang van de schadevergoeding zal vaak gering zijn en bovendien lastig te bewijzen. Zowel consumenten als ondernemers doen er dan ook verstandig aan alternatieven achter de hand te hebben.

## 1. Inleiding

We hebben het allemaal gemerkt: de Nederlandse banken zijn afgelopen voorjaar blootgesteld aan gedurige aanvallen via internet, die ertoe leidden dat hun elektronische dienstverlening haperde of geruime tijd zelfs niet beschikbaar was. In een Vooraf<sup>2</sup> heeft Corien Prins enkele vragen opgeworpen die men naar aanleiding hiervan kan stellen. In dit artikel zal ik proberen hier enige antwoorden op te formuleren. Allereerst is van belang om te weten wat er nu eigenlijk technisch gezien aan de hand is: dit wordt in het artikel van prof. B. Jacobs<sup>3</sup> besproken; ik zal hier kort in par. 4 op terugkomen.

Om de juridische vragen te beantwoorden zal ik drie onderwerpen aansnijden: zorgplichten en remedies bij dienstverlening, zorgplichten van banken, en zorgplichten rond internet. Vervolgens zal ik op basis van die discussie het eigenlijke onderwerp van dit artikel behandelen. Ik merk op dat ik mij concentreer op dat wat de banken zelf kunnen doen. Daarom ga ik bijvoorbeeld niet in op IPR-vragen of andere internationale kwesties: de aansprakelijkheid van de daders is een ander onderwerp. Verder ga ik niet in op de algemene sociale gevolgen, behalve voor zover dat relevant is voor de juridische analyse.

## 2. Zorg en contractuele aansprakelijkheid algemeen

De aansprakelijkheid voor niet-beschikbare contractueel overeengekomen diensten wordt primair bepaald aan de hand van de vraag of een externe oorzaak van niet-nakoming toerekenbaar is in de zin van art. 6:74 BW. Die toerekenbaarheid moet worden bepaald op basis van art. 6:75 BW, dat verwijst naar schuld, wet, rechtshandeling en verkeersopvattingen. Achter dit stelsel ligt de gedachte dat men moet bepalen of de oorzaak van de niet-nakoming overmacht uitmaakt (wat wil zeggen, *niet* toerekenbaar is). Bij een externe oorzaak werkt dit als volgt uit.

Eerst moet worden gezien of er een voorzorgsmaatregel bestond en of die in casu geleverd kon worden: als dat zo is, is er sprake van schuld (verwijtbaar tekortschieten in de vereiste zorg). Als er geen effectieve voorzorgsmaatregel geleverd mocht worden, vormt de externe oorzaak 'overmacht', tenzij de oorzaak op andere grond

toerekenbaar is (en dus aan de schuldenaar kan worden toegerekend, voor diens risico komt).<sup>4</sup> Of zij op andere grond toerekenbaar is, moet worden beoordeeld aan de hand van uitleg van de overeenkomst (de rechtshandeling), naast verkeersopvattingen en wettelijke normen, zoals normen omtrent de omvang van de vereiste zorg (bijvoorbeeld art. 7:401 BW).

Voor de invulling van de vereiste mate van zorg en het toegerekende risico zullen daarnaast van belang zijn wat daadwerkelijk geleverd kan worden, en (in elk geval bij commerciële verhoudingen) hoe de risico's zijn afgewogen. Immers als men een hogere mate van zorg wenst of meer risico bij de schuldenaar wil leggen zal daar in het algemeen ook een hogere prijs voor moeten worden betaald. Een voorbeeld is het aangetekend per post versturen van kostbare zaken. Economisch gezien gaat het erom hoeveel de schuldeiser bereid is te betalen voor een zeker niveau van zorg: een bedrijf zal in commerciële verhoudingen immers de kosten verdisconteren in de prijs en dit daarom doorberekenen aan de klant, en de klant zal volgens de wetten van de markt zoeken naar het product met de gewenste eigenschappen tegen de laagste prijs, en daarmee dus het door hem gewenste niveau van zorg bepalen.<sup>5</sup>

Daarbij moet worden bedacht dat in veel gevallen de schuldeiser allerminst prijs stelt op het allerhoogste niveau van zorg als hij daarvoor moet betalen. Dat kan zijn omdat het voorwerp tegen een stootje kan, of de waarde ervan gering is. Ook is mogelijk dat de schuldeiser waar nodig zelf extra voorzorgsmaatregelen of schadebe-

**In veel gevallen stelt de schuldeiser allerminst prijs op het allerhoogste niveau van zorg als hij daarvoor moet betalen**

perkende voorzieningen kan treffen. Wellicht zijn de schadelijke gevolgen zodanig verdeeld dat deze beter bij de schuldeiser kunnen worden opgevangen voor zover deze het wenst. Zo hebben ziekenhuizen een noodaggregaat voor als de stroom uitvalt; gewone burgers vinden zulke maatregelen te duur voor wat het oplevert. Dit is een economisch efficiënt stelsel.

Daarnaast is van belang of er een adequate remedie is bij wanprestatie. Bij dienstverlening speelt dit met name omdat de typische schade daar meestal zogenaamde gevolgschade is, waar veelal voor geëxonerend wordt. Overigens is het ook mogelijk om als remedie te ontbinden en gedeeltelijke terugbetaling van het loon te verkrijgen.<sup>6</sup> Dit levert evenwel geen vergoeding van gevolgschade op.

Bij sommige diensten, met name die welke een belangrijke maatschappelijke functie vervullen (zoals bij beroepen als de arts of de notaris), gelden ter bescherming van de opdrachtgever additionele regels. Enerzijds zijn daar veelal zwaarwegende en bijzondere zorgplichten aangenomen die tot een hoger niveau van zorg leiden.<sup>7</sup> Anderzijds zijn exoneraties daar slechts beperkt toegestaan.<sup>8</sup> Daarnaast onderscheidt men ook diensten van algemeen belang:<sup>9</sup> deze zijn onontbeerlijk voor burgers, reden waarom daar bijzondere regels voor worden gesteld. Een voorbeeld is de dienstverlening die bestaat uit energieleveranties.<sup>10</sup> Voor elektriciteitsleverantie is er bijvoorbeeld een publieke regeling die in geval van stroomuitval van zekere duur de leverancier verplicht tot uitbetaling van forfaitaire compensatievergoedingen aan afnemers.<sup>11</sup> Dit vergemakkelijkt het verkrijgen van compensatie, en lijkt daarnaast een zekere drempel aan te leggen voor vorderingen van volledige schade (zodat de leverancier ook zijn risico's beter kan inschatten). Eenzelfde type regeling is voor telecomdiensten voorgesteld.<sup>12</sup> De overheid heeft met dergelijke regelingen tevens zekere beschikbaarheidseisen voor de dienst geformuleerd. Dit is een ander aspect van maatschappelijk belangrijke diensten: individuen hebben belang bij de beschikbaarheid ervan.<sup>13</sup>

### 3. Zorgplichten bij banken

In jurisprudentie en literatuur is aanvaard dat op banken tamelijk verstrekkende zorgplichten rusten.<sup>14</sup> Deze zijn gebaseerd op de maatschappelijke positie van banken. Zij

brenge met zich dat banken niet geheel de belangen van anderen (in het bijzonder hun cliënten) ondergeschikt mogen maken aan hun eigen belangen, en nadrukkelijker moeten wijzen op risico's. Dit toont zich bijvoorbeeld in strengere eisen aan voorlichting aan cliënten en eventuele potentiële cliënten,<sup>15</sup> grotere eerlijkheid bij geschillen,<sup>16</sup> en meer algemeen het ondergeschikt maken van het eigen belang. Daarnaast dient de zorgplicht uiteraard ook de kwaliteit van de dienstverlening zelf: de dienstverlener moet zijn werk goed doen.

De beschikbaarheid van de dienstverlening is evenwel zelden voorwerp van discussie. Toch kan men, gelet op het belang van bancaire dienstverlening voor het maatschappelijk verkeer vandaag de dag, betogen dat ook voor de beschikbaarheid van bancaire diensten hogere zorgplichten gelden dan bij gewone contractuele relaties. Een indicatie hiervoor is de discussie die ontstaat wanneer banken additionele selectiecriteria opleggen aan potentiële cliënten, bijvoorbeeld door minder snel hypotheek in bepaalde wijken te verstrekken, of door minder

## Bancaire diensten worden inmiddels door velen als dienst van algemeen maatschappelijk belang beschouwd

wenselijke cliënten te weigeren.<sup>17</sup> Die discussie laat zien dat bancaire diensten inmiddels door velen als dienst van algemeen maatschappelijk belang worden beschouwd, wat zou impliceren dat er contractdwang en een grote mate van daadwerkelijke beschikbaarheid vereist is.

Bij internetbankieren (om dit als verzamelterm te nemen) worden evenwel specifieke voorwaarden gehanteerd om aansprakelijkheidsrisico's te beperken. Zo wordt wel gestipuleerd dat de dienstverlening zonder vooraankondiging kan worden opgeschort bij storingen of dat ongestoorde dienstverlening niet gegarandeerd is,<sup>18</sup> en wordt geëxonerend voor schade als gevolg van niet-

#### Auteur

1. Prof. mr. T.F.E. Tjong Tjin Tai is hoogle-  
raar privaatrecht, Tilburg University.

#### Noten

2. *NJB* 2013/948, afl. 18, p. 1185
3. 'De DDoS Paradox: Ontsluiten door Afsluiten', *NJB* 2013/1968, afl. 32, p. 2191-2195
4. Zie in meer detail T.F.E. Tjong Tjin Tai, 'Toerekenbare niet-nakoming en de zorg van een goed schuldenaar', *WPNR* 6574 (2004), p. 285-290, ook G.T. de Jong, *Niet-nakoming van verbintenissen*, Mon. BW B33, 2006, nr. 14 en 19.4, Asser/Hartkamp & Sieburgh 6-1\*, nr. 340, 344.
5. Althans volgens de klassieke economi-

sche theorie, en behoudens verstoringen op de markt.

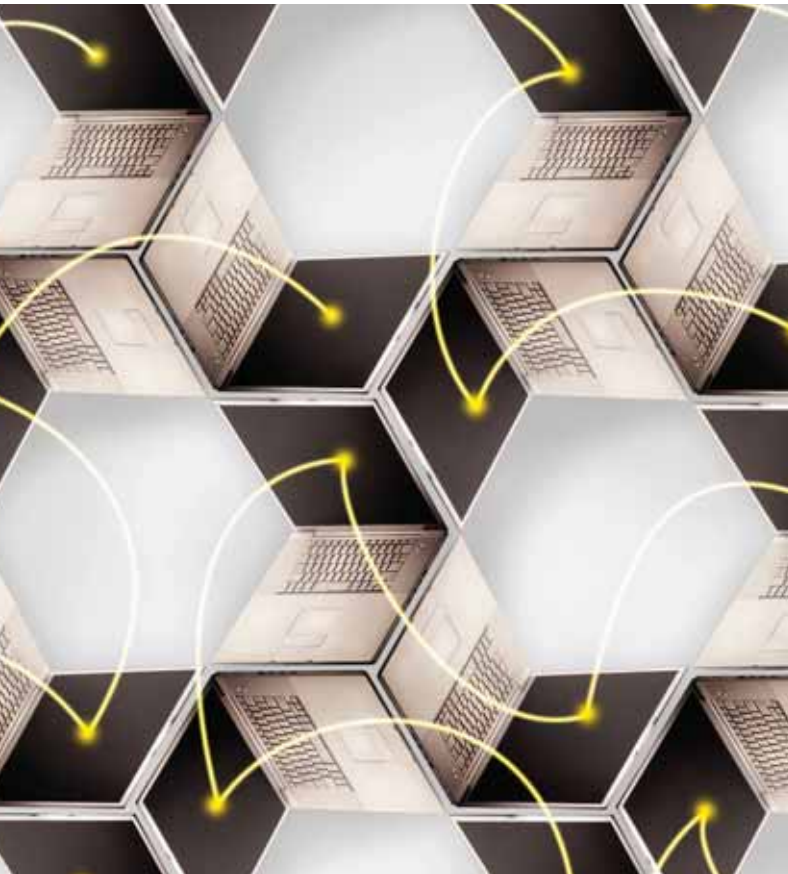
6. HR 29 maart 2002, *NJ* 2002/270.
7. T.F.E. Tjong Tjin Tai, *Zorgplichten en zorgethiek*, diss. Amsterdam (UvA) 2007, hfdst. 6.
8. Bijv. art. 7:453 BW voor geneeskundige behandelingen, ook beroepsregels voor advocaten e.d.
9. Communicatie Commissie 20 december 2011, COM(2011)900def.
10. COM(2011)900def. beschouwt dit als dienst, evenzo M.B.M. Loos, *De energieleveringsovereenkomst*, diss. Utrecht 1998, p. 74-77.
11. Art. 31 lid 1 sub f Elektricitwet 1998 juncto art. 6.3.1 Netcode Elektriciteit. Ver-

gelijk HR 29 april 2011, *LJN* BQ2935, *NJ* 2011/191 (*Bouwcombinatie/Liander*), r.o. 3.3.3.

12. <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2013/05/22/brief-aan-de-tweede-kamer-compensatie-bij-storingen-in-de-telecomsector/brief-aan-de-tweede-kamer-compensatie-bij-storingen-in-de-telecomsector.pdf>
13. Dit verklaart het bestaan van contractdwang in dergelijke gevallen, waarover I. Houben, *Contractdwang*, diss. Leiden 2005.
14. De literatuur is overvloedig; ik zie af van verwijzingen.
15. Bijv. HR 5 juni 2009, *NJ* 2012/182-184 (*Effectenlease*).

16. Bijv. HR 29 september 1995, *NJ* 1998/81 (*ABN AMRO/Hendriks*).

17. Dat kan dan gaan om cliënten die worden verdacht van criminele banden en/of betrokkenheid bij prostitutie, zie bijvoorbeeld *Volkskrant* website 6 februari 2009, <http://www.volkskrant.nl/vk/nl/2680/Economie/article/detail/314691/2009/02/06/Geen-zaken-met-uitschot.dhtml>.
18. Art. 2 lid 4 Voorwaarden Mijn SNS versie 1 jan 2012, vergelijk Hfdst 4, art. 4 lid 1 Algemene voorwaarden voor betaalkeningen en betaaldiensten Rabobank 2013, evenzo de diverse voorwaarden van ABN AMRO (er gelden verschillende voorwaarden voor verschillende producten en voor consumenten en bedrijven).



Computernetwerk © Hollandse Hoogte

beschikbaarheid of storingen.<sup>19</sup> Op zichzelf valt te begrijpen dat banken vroeger weinig zekerheid boden: internetbankieren was ooit een extra facilititeit bovenop de gewone dienstverlening. Inmiddels is echter internetbankieren de voornaamste toegang tot het betalingsverkeer geworden, en bovendien stimuleren banken zelf dat klanten uitsluitend van internetbankieren gebruik gaan maken. Dan mogen zij ook werk maken van continue beschikbaarheid.

#### 4. Internet

Ten slotte is er de derde categorie zorgplichten: zorgplichten rond internet. Bij dit onderwerp ligt de nadruk op twee aspecten: de vraag wanneer men met internet zelf schadelijke handelingen verricht, en de vraag in hoeverre men inbreuken door anderen moet verhinderen.<sup>20</sup> Het gaat nu om een andere vraag: in hoeverre moet men waken tegen inbreuken door derden? Dit is in essentie de vraag wanneer een beletsel voor nakoming toerekenbaar is, dan wel overmacht vormt. Zoals in par. 2 aangegeven is dit een vraag naar de te vergen mate van zorg, naast toerekening van niet te vermijden risico's.

Een DDoS-aanval wordt gerealiseerd,<sup>21</sup> voorzover ik begrijp, doordat iemand via zijn computer een 'botnet' gebruikt, bestaande uit een groot aantal computers van onwetende individuen die na infectie door een computervirus o.i.d. onder controle staan van de botnetbeheerder. Op commando van de beheerder gaan deze computers zeer veel verzoeken sturen naar de server van een bepaalde website. Omdat servers slechts een begrensde hoeveelheid verzoeken aankunnen, is het gevolg overbelasting, waardoor de server uitvalt en de website onbereikbaar wordt.

Maatregelen hiertegen lijken niet zo eenvoudig te zijn. Krachtiger servers helpen niet tegen een echt grote aanval; het gebruikmaken van backup systemen elders is wellicht lastig omdat het van belang is dat er één correcte administratie is.<sup>22</sup> Wel is het zaak dat de servers (en software) zo goed mogelijk ingericht zijn, aangezien DDoS-aanvallen regelmatig ook gebruikmaken van softwarefouten waardoor de servers sneller uitvallen. Andere maatregelen zijn bijvoorbeeld het gebruikmaken van filters die proberen de aanval te onderscheiden van serieuze verzoeken.

#### 5. Banken en aansprakelijkheid bij DDoS-aanvallen

In hoeverre valt er juridisch iets te zeggen over wat van banken mag worden verwacht? Het gaat dan om drie punten:

- is er een verplichting om maatregelen te nemen tegen DDoS-aanvallen?
- levert een DDoS-aanval overmacht op?
- is er reden van de gewone regels af te wijken?

##### 5.1 Een zorgplicht voor beschikbaarheid van internetbankieren?

De in par. 3 genoemde bancaire voorwaarden suggereren dat internetbankieren niet gegarandeerd beschikbaar is, en door de bank buiten werking kan worden gesteld wanneer de bank dat goeddunkt, in elk geval bij een storing. De klant zou dus geen recht hebben op beschikbaarheid van internetbankieren. Er kan echter worden betwist of dit zonder meer geldt. De beschikbaarheid lijkt immers centraal te staan bij de dienst, terwijl het bovendien gaat om een dienst die tegenwoordig essentieel is voor het gebruik van betaalrekeningen. Een beding dat de bank het recht geeft om naar believen een verplichting niet na te komen is onredelijk bezwarend ex art. 6:236 sub a BW, vergelijk ook art. 6:237 sub b BW over wezenlijke beperking van de prestatie. Dat zou te meer gelden nu het lijkt te gaan om een dienst van algemeen belang.

Het is daarom verdedigbaar (al is dat niet geheel zeker), dat banken verplicht zijn zorg te dragen voor ongestoorde dienstverlening. Daaruit vloeit voort dat er redelijke voorzorgsmaatregelen tegen storing – inclusief storing als gevolg van DDoS-aanvallen – moeten worden genomen. Het artikel van Jacobs geeft aan dat er best nog wel wat mogelijk is. Daar staat echter tegenover dat het onmogelijke noch het onredelijke verwacht mogen worden. Storingen kunnen nooit geheel worden uitgesloten, terwijl disproportionele maatregelen eveneens niet verwacht mogen worden. Het lijkt niet wenselijk dat banken enorme kosten gaan maken die door alle klanten gezamenlijk moeten worden betaald als de daarmee voorkomen schade voor veel klanten<sup>23</sup> gering is. Meer voor de hand ligt dan om te werken met alternatieven, zoals een apart, robuuster noodnetwerk dat alleen kan worden gebruikt door klanten die bereid zijn meer te betalen voor een hoger niveau van beschikbaarheid.<sup>24</sup> Klanten die dat niet willen, zullen veelal zelf alternatieve maatregelen kunnen treffen, zoals het houden van een voldoende voorraad contant geld, gebruikmaken van credit cards of PayPal.<sup>25</sup> Ook bedrijven als webwinkels kunnen alternatieve betaalwijzen toelaten en zich daardoor minder kwetsbaar maken. Overigens zij toegeven dat banken zelf ook proberen om de klant af te houden van het gebruik van



contant geld. Nochtans blijft voorop staan dat een gedistribueerde aanval het beste kan worden opgevangen door gedistribueerde voorzorgsmaatregelen.

Dit is overigens een algemene zwakte van het geloof in internet en netwerken:<sup>26</sup> men ziet over het hoofd dat de techniek onvermijdelijk af en toe uitvalt. We behoren dan een alternatief of vangnet te hebben om ernstige gevolgen te vermijden. Dit vergt zowel een technisch

## Een zekere mate van autarkie, in de vorm van fysieke en/of lokale voorzieningen, is ook in de netwerksamenleving nodig

ontwerp volgens klassieke ingenieursdeugden,<sup>27</sup> als een beperkter vertrouwen op de techniek van de zijde van de klanten. Een zekere mate van autarkie, in de vorm van fysieke en/of lokale voorzieningen, is ook in de netwerksamenleving nodig. Het zou goed zijn als bestuurders in overheid en zakenleven doordrongen zouden raken van het belang van decentrale robuustheid, en leren om kritisch te staan tegenover adviseurs die benadrukken dat het in 99,99% van de gevallen goed gaat.

### 5.2 Vormt een DDoS-aanval overmacht?

Ook als er geen zorgplicht is geschonden, blijft mogelijk dat banken in bepaalde gevallen toch aansprakelijk zijn: de oorzaak van de tekortkoming is dan zonder verwijtbaarheid toerekenbaar. Zo'n uitkomst kan men verklaren met een economisch getinte overweging: de bank bespaart weliswaar kosten door bepaalde schade niet te voorkomen, maar het kan onredelijk zijn om die schade dan eenzijdig af te wentelen op de klanten die toevallig daarmee geconfronteerd worden.<sup>28</sup> Het is billijker om die schade over het collectief om te slaan en dus in de kostprijs door te berekenen. Een DDoS-aanval raakt evenwel vrijwel alle klanten,

zodat deze ratio niet opgaat. Wel kan men een vergelijkbare redenering volgen, namelijk: soms is het goedkoper en passender om een redelijke schadevergoeding te betalen dan voorzorgsmaatregelen te treffen. Dat geldt met name bij voorvallen die voor de dienstverlener slechts tegen zeer hoge kosten te vermijden zijn en die normaliter geen grote schade opleveren.<sup>29</sup> Of dit evenwel in concreto passend is, vergt toepassing van art. 6:75 BW: kan worden toegerekend op basis van rechtshandeling, wet of verkeersopvattingen? Naar geldend recht lijkt dit bij DDoS-aanvallen niet zonder meer het geval. In het bijzonder hebben banken veelal bij overeenkomst gestipuleerd dat storingen niet toerekenbaar zijn, dus overmacht vormen, dan wel dat ongestoorde communicatie niet overeengekomen is.

Zowel wat betreft de omvang van de beschikbaarheid als de omvang van de schadevergoeding worden door banken in hun voorwaarden contractuele beperkingen geformuleerd. Deze gelden tenzij deze in concrete gevallen geen gevolg hebben. Zulke bedingen zijn op zichzelf niet onredelijk bezwarend;<sup>30</sup> derhalve kan hoogstens de derogerende werking van redelijkheid en billijkheid aan een beroep hierop in de weg staan. De omstandigheid dat het gaat om een dienst van groot algemeen maatschappelijk belang zou dit tot op zekere hoogte kunnen rechtvaardigen; het blijft evenwel lastig te voorspellen hoe de Hoge Raad hier in voorkomend geval over zou oordelen. Op zichzelf is denkbaar<sup>31</sup> dat wordt aangenomen dat er wel een zekere verplichting bestaat om zorg te dragen voor beschikbaarheid, echter de uitsluiting van schadevergoeding (behoudens opzet en bewuste roekeloosheid) zal gelet op de desbetreffende rechtspraak van de Hoge Raad<sup>32</sup> waarschijnlijk overeind blijven.

### 5.3 Afwijking van de gewone regels?

Het lijkt er dus vrij somber uit te zien vanuit strikt juridisch perspectief. Er zijn evenwel een paar kanttekeningen en aanvullingen op hun plaats die maken dat de gewone analyse misschien niet onverkort geldt.

Allereerst – schrale troost – is het los van toerekenbaarheid mogelijk om de remedie van gedeeltelijke ontbinding in te roepen, en op die basis gedeeltelijke terugbetaling van de kosten van de dienst te verkrijgen.<sup>33</sup> Dit levert evenwel praktisch niets op nu deze kosten laag zijn.

Daarnaast kan er wellicht vanuit ander perspectief

19. Art. 9 sub b Voorwaarden Mijn SNS, art. 24.1 Voorwaarden Mijn ING jan 2013 (behoudens opzet/grove schuld), hfdst. 3, art. 18 lid 2 Voorwaarden Rabobank, evenzo ABN AMRO.

20. Dit betreft meestal de zorgplicht van Internet dienstverleners (ISPs), waarvoor art. 6:196C BW bepaalt dat in bepaalde gevallen (onwetendheid en neutraliteit) in elk geval geen aansprakelijkheid bestaat, en voor het overige het algemene onrechtmatige daadsrecht bepalend is. Zie nader bijv. B. Van der Sloot, 'De verantwoordelijkheid voorbij: de ISP op de stoel van de rechter', *Tijdschrift voor Internetrecht* 2011/5, p. 136-140, IVIR-rapport 'Op weg naar evenwicht. Een onderzoek naar zorgplichten op

het internet', juni 2010.

21. In de navolgende paragraaf zal ik de zaken versimpelen: als ik dit technisch precies correct zou formuleren zou ik vermoedelijk voor niet-gespecialiseerde juristen onbegrijpelijk zijn.

22. Dit onderscheidt de bank van Google, die de zoekmachine over meerdere systemen kan verspreiden omdat de benodigde database op meer plaatsen aanwezig kan zijn.

23. Consumenten en bedrijven.

24. Vergelijk de mogelijkheid dat er een back-up mogelijkheid komt voor PIN-betalen in geval van storing van het gewone netwerk; dit is er kennelijk al in België, zie <http://www.dedetailhandel.nl/>

nieuws/2013/369.

25. Zie ook het artikel van Jacobs.

26. Zoals in de wens om kantoorsoftware en documenten 'in the cloud' te delen.

27. Vergelijk de mogelijkheden genoemd in het artikel van Jacobs.

28. Vergelijk de 'égalité pour les charges publiques' bij overheidsaansprakelijkheid, of de regeling inzake productenaansprakelijkheid.

29. Bovendien geldt ook hier dat het zinvol kan zijn dat de afnemer die daar belang bij heeft zelf extra voorzorgsmaatregelen treft, vergelijk een noodaggregaat bij stroomuitval.

30. Behoudens de exonatie, vergelijk art. 6:237 sub f BW, waarover hierna aan het

slot van par. 5.2.

31. Er is op dit punt nauwelijks jurisprudentie, terwijl er een groot maatschappelijk belang is: er lijkt mij daarom een mogelijkheid te zijn dat de Hoge Raad in deze zin zou oordelen.

32. Laatstelijk HR 17 februari 2012, *LJN* BU9891, verder Asser/Hartkamp & Sieburgh 6-1\* (2012), nr. 364-369, Duyvensz, *WPNR* 6878 (2011), Wessels/Jongeneel/Hendrikse, Algemene voorwaarden, 5e dr., 2010, par. 14.6.2 en de interessante analyse in par. 14.7, waar de hier verdedigde benadering bij lijkt aan te sluiten.

33. HR 29 maart 2002, *NJ* 2002/270.

naar worden gekeken. In het Europees recht wordt in sterkere mate dan naar Nederlands recht gewerkt met de gedachte dat regelgeving bepaalde rechten toekent, welke rechten daadwerkelijk effectief moeten zijn.<sup>34</sup> Er mag dan niet door andere regels, zoals vervaltermijnen of procedurele beperkingen, afbreuk worden gedaan aan deze rechten. In casu gaat het om een dienst van algemeen belang, waarvan nodig is dat deze effectief beschikbaar is. Dit vereist daadwerkelijk maatregelen voor het verzekeren van de beschikbaarheid, en daarom ook juridische voorzieningen om tot zulke beschikbaarheid aan te zetten (prikkel). Hiertoe behoren remedies ingeval van tekortschieten. Als het gemeene recht onvoldoende remedies biedt dan wel drempels in de weg legt, zullen er aanpassingen nodig zijn. Zo'n redenering dient te berusten op een Europese regeling die een 'recht' geeft op beschikbaarheid van internetbankieren.<sup>35</sup>

In casu is er zo'n regeling: de Richtlijn betalingsdiensten 2007/64/EG, geïmplementeerd in art. 7:514-551 BW. Deze regels verplichten de dienstverlener – dwingendrechtelijk, art. 7:550 BW – tot betalen van schadevergoeding indien een betaling niet of gebrekkig wordt uitgevoerd (art. 7:543-546 BW). Deze verplichting geldt overigens niet 'in abnormale en onvoorziene omstandigheden die onafhankelijk zijn van de wil van degene die zich erop beroept en waarvan de gevolgen ondanks alle voorzorgsmaatregelen niet konden worden voorkomen' (art. 7:548 BW): ook hier geldt dus een uitzondering voor overmacht. Alhoewel de regels niet expliciet ook gelden voor het geval dat de klant

## De omvang van de schadevergoeding zal vaak gering zijn

een betalingsinstructie niet kan doorgeven doordat de server van de bank onbereikbaar is, lijken de regels zich wel hiertoe uit te strekken. Een dergelijke extensieve uitleg heeft het HvJ EG wel vaker laten zien ten behoeve van consumenten.<sup>36</sup> Hier zou dat op zijn plaats zijn omdat anders de rechten van de consument te gemakkelijk kunnen worden uitgehold. De exonaties en beperkingen van de zorgplicht zouden op deze grond wellicht dus toch opzij kunnen worden geschoven, zo niet geheel dan toch gedeeltelijk.

Dit wijst er dus op dat de consument niettegenstaande de bancaire voorwaarden recht heeft op schadevergoeding als de bank onbereikbaar was, tenzij de bank dit echt niet kon helpen. Een 'maar' blijft hier wel bestaan: in veel gevallen zal het nog niet zo eenvoudig zijn om daadwerkelijk significante schade aan te tonen. De niet-betaling van schulden voor enkele dagen leidt niet snel tot grote schade.<sup>37</sup> Grote ergernis van consumenten wordt door de Hoge Raad niet op geld gewaardeerd.<sup>38</sup>

Voor een webwinkel ligt dit anders.<sup>39</sup> Een webwinkel waarbij enige tijd niet betaald kan worden met iDeal en die daarom verkopen mist, kan op zichzelf wel substantiële winst derven. Toch is dit niet geheel zeker: als alle Nederlandse webwinkels dit probleem hebben, kunnen zij alleen naar een fysieke concurrent gaan. Het is daarom zeer wel mogelijk dat de inkopen worden uitgesteld en na

de DDoS-aanval alsnog worden gedaan. Daarnaast geldt de hierboven beschreven redenering ten aanzien van de Richtlijn betalingsdiensten niet voor bedrijven: het is daarom zeer de vraag of bedrijven onder de exonaties en beperkingen van de zorgplicht uit kunnen komen.

Als laatste is er bij webwinkels een complicatie in de rechtsverhoudingen. Het is mij niet precies duidelijk of bij een DDoS-aanval de winkel die daar last van heeft ook noodzakelijk klant is van de aangevallen bank. Het is voorstelbaar dat een DDoS-aanval op ING tot gevolg heeft dat een klant van ING niet kan betalen bij een bedrijf dat bij Triodos bankiert, maar dat een klant van ABN dat wel kan. Voor de aansprakelijkheid zou de Triodos-webwinkel zich dan tot ING moeten richten op basis van onrechtmatige daad in plaats van overeenkomst, en loopt dan aan tegen de vraag of de contractuele zorgplicht van ING jegens haar klanten ook doorwerkt jegens derden. Het voert te ver om hier ook nog op deze vraag in te gaan.

Een derde mogelijkheid is dat de wetgever ingrijpt. Een alternatieve benadering zou zijn om net als bij veel diensten van algemeen belang te werken met een forfaitaire schadevergoeding bij storingen.<sup>40</sup> Daar is evenwel een specifieke wettelijke regeling voor nodig; gelet op de verregaande harmonisatie van financiële dienstverlening in Europa is het mogelijk dat dit Europese regelgeving zal vergen. Het voordeel van zo'n regeling is wel dat het voor klanten van de banken veel gemakkelijker wordt om schadevergoeding te verkrijgen.

### 6. Tot besluit

Uit het voorgaande blijkt dat ik gematigd optimistisch ben over de *mogelijkheid* om bij banken claims in te dienen voor schadevergoeding wegens niet-beschikbaarheid van Internetbankieren. De *omvang* van de schadevergoeding zal echter vaak gering zijn en bovendien lastig te bewijzen. Ingrijpen door de wetgever biedt dan nog de beste oplossing, al is onzeker of dit er daadwerkelijk van zal komen.

Dit lijkt wellicht een teleurstellende conclusie, met name als men zich er zorgen over maakt of banken wel genoeg proberen te doen om verdere aanvallen te voorkomen. Nochtans is dat de uitkomst van een zakelijke analyse van het geldend recht. Dit hoeft uit preventief oogpunt niet bezwaarlijk te zijn; naast juridische prikkels is de reputatieschade die banken dreigen te lijden bij DDoS-aanvallen een niet onbelangrijke aanzet tot actie. •

34. Men spreekt van het effectiviteitsbeginsel, zie met verwijzingen T.F.E. Tjong Tjin Tai, 'Effectiviteitsbeginsel en nationaal privaatrecht', *WPNR* 6901 (2011), p. 790-797.

35. Immers naar Nederlands recht kennen we niet een effectiviteitsbeginsel.

36. Zie bijvoorbeeld HvJ EG 30 april 2002, nr. C-400/00 (*Club-Tour vs. Garrido*) waarbij de reikwijdte van de Richtlijn pakketreizen werd uitgebreid, of de rechtspraak inzake vergoeding wegens vertraging bij passagiersvluchten. Het voert te ver dit gedetailleerd uit te werken.

37. Bovendien zou een DDoS-aanval moge-

lijk overmacht kunnen opleveren.

38. Vergelijk HR 5 december 2008, *NJ* 2010/579 (*Pollen vs. Linssen*).

39. Voor andere bedrijven lijkt evenmin snel sprake van grote schade als zij een tijd geen betalingen kunnen doen of ontvangen. Bovendien kunnen die waarschijnlijk nog langs andere kanalen hun bank opdrachten geven.

40. Vergelijk opinie Nijboer, *Volkskrant* website 19 juni 2013, <http://www.volkskrant.nl/vk/nl/3184/opinie/article/detail/3460984/2013/06/19/Storing-Geld-moet-ook-online-altijd-veilig-en-beschikbaar-zijn.dhtml>